



TEKNOLOGISK  
INSTITUT

Online kursus – k72746

---

# Cybersecurity Collection

---

Title	Estimated Duration (hrs)
TestPrep 300-208 Implementing Cisco Secure Access Solutions (SISAS)	1,50
Cloud System Architecture – Concepts and Design	2,20
Cloud Data Security	1,90
Cloud System Security - Platform and Infrastructure	2,00
Cloud Application Security	2,20
Cloud Service – Operations Management	3,00
Cloud Service – Legal and Compliance	2,10
CompTIA Cybersecurity Analyst+ CS0-001: Network Architecture and Reconnaissance	3,10
CompTIA Cybersecurity Analyst+ CS0-001: Threat Identification	2,40
CompTIA Cybersecurity Analyst+ CS0-001: Threat Mitigation	2,20
CompTIA Cybersecurity Analyst+ CS0-001: Reducing Vulnerabilities	2,40
CompTIA Cybersecurity Analyst+ CS0-001: Investigate Security Incidents	2,20
CompTIA Cybersecurity Analyst+ CS0-001: Monitoring for Security Issues	2,30
CompTIA Security+ SY0-501: The Present Threat Landscape	0,90
CompTIA Security+ SY0-501: Types of Malware	0,90
CompTIA Security+ SY0-501: Social Engineering and Related Attacks	0,70
CompTIA Security+ SY0-501: Application and Service Attacks	0,90
CompTIA Security+ SY0-501: Cryptographic and Wireless Attacks	0,80
CompTIA Security+ SY0-501: Penetration Testing and Vulnerability Scanning	0,80
CompTIA Security+ SY0-501: Impacts from Vulnerability Types	0,90
CompTIA Security+ SY0-501: Components Supporting Organizational Security	1,50
CompTIA Security+ SY0-501: Security Assessment Using Software Tools	0,90
CompTIA Security+ SY0-501: Cryptography	2,00
CompTIA Security+ SY0-501: Public Key Infrastructure	1,10
CompTIA Security+ SY0-501: Wireless Security Settings	1,30
CompTIA Security+ SY0-501: Analyzing Output from Security Technologies	1,00
CompTIA Security+ SY0-501: Deploying Mobile Devices Securely	0,50
CompTIA Security+ SY0-501: Implementing Secure Protocols	0,50
CompTIA Security+ SY0-501: Troubleshooting Common Security Issues	0,40
CompTIA Security+ SY0-501: Identity Concepts and Access Services	0,60
CompTIA Security+ SY0-501: Identity and Access Management Controls	0,50
CompTIA Security+ SY0-501: Common Account Management Practices	0,60
CompTIA Security+ SY0-501: Frameworks, Guidelines, and Physical Security	2,00
CompTIA Security+ SY0-501: Implement Secure Network Architecture Concepts	0,80
CompTIA Security+ SY0-501: Secure System and Application Design and Deployment	1,50
CompTIA Security+ SY0-501: Cloud, Virtualization, and Resiliency Concepts	1,10
CompTIA Security+ SY0-501: Policies, Plans, and Procedures	0,80
CompTIA Security+ SY0-501: Business Impact Analysis and Risk Management	1,10
CompTIA Security+ SY0-501: Incident Response, Forensics, and Disaster Recovery	1,10
IT Security for End Users: IT Security Fundamentals	0,90
IT Security for End Users: Using Corporate Devices Securely	0,80
IT Security for End Users: Secure Corporate Communications and Networking	0,80
Microsoft SharePoint Server 2013 - Developing Core Solutions: Implement Security	1,60

IINS 3.0: Introduction to Cisco Security	0,80
IINS 3.0: SIEM Technology and Security Terminology	1,20
IINS 3.0: Introduction to Network Attacks	1,10
IINS 3.0: Specific Network Attacks	0,60
IINS 3.0: Malware and Data Loss	1,20
IINS 3.0: Encryption Methods	0,90
IINS 3.0: Cryptographic Key Exchange	1,00
IINS 3.0: Network Topologies	1,20
IINS 3.0: Secure Device Management	0,50
IINS 3.0: Auto Secure	0,80
IINS 3.0: Management Plane Access	0,90
IINS 3.0: Simple Network Management Protocol	0,60
IINS 3.0: Network Time Protocol	0,80
IINS 3.0: SCP and AAA Technologies	1,00
IINS 3.0: TACACS+	0,90
IINS 3.0: Network Access Control	1,00
IINS 3.0: Port Based Access Control, BYOD, and MDM	1,00
IINS 3.0: IPsec and VPN	1,00
IINS 3.0: Clientless SSL VPN & ASDM	0,60
IINS 3.0: AnyConnect VPN Using ASDM	1,10
IINS 3.0: IPsec Site-to-Site VPN	1,00
IINS 3.0: Secure CLI Access	0,60
IINS 3.0: OSPF and EIGRP Authentication	1,10
IINS 3.0: Attack Mitigation	1,50
IINS 3.0: Control Plane Policing	0,50
IINS 3.0: PVLANS and VLAN Security	1,00
IINS 3.0: Firewall Technology	0,60
IINS 3.0: Network Address Translation	0,90
IINS 3.0: Zone-Based Firewall Configuration	0,80
IINS 3.0: ASA Security and Policies	1,40
IINS 3.0: Firewall Features	0,60
IINS 3.0: IPS Deployment Configuration	1,10
IINS 3.0: Configuring Cisco IPS	0,90
IINS 3.0: Threat Mitigation for Email, Web, and Endpoints	1,30
CompTIA PenTest+: Planning for an Engagement	0,90
CompTIA PenTest+: Scoping an Engagement	0,90
CompTIA PenTest+: Information Gathering	0,90
CompTIA PenTest+: Vulnerability Identification	0,70
CompTIA PenTest+: Social Engineering and Specialized System Attacks	0,90
CompTIA PenTest+: Network-Based Exploits	1,30
CompTIA PenTest+: Application-Based Vulnerabilities	0,90
CompTIA PenTest+: Local Host Vulnerabilities	0,60
CompTIA PenTest+: Post-Exploitation and Facilities Attacks	0,70
CompTIA PenTest+: Penetration Testing Tools	1,40
CompTIA PenTest+: Analyzing Tool and Script Output	0,90

CompTIA PenTest+: Reporting and Communication	0,60
SECFND: Overview and Network Models	0,60
SECFND: Network Models	0,90
SECFND: Basic Networking Protocols	1,00
SECFND: Basic Networking Services	1,00
SECFND: Network Devices Operations & Security	1,20
SECFND: Network Addressing	0,90
SECFND: VLANS and Data Visibility	0,50
SECFND: ACLs & Filtering	0,90
SECFND: Filtering and Packet Capture	1,00
SECFND: Packet Analysis	0,80
SECFND: Data Loss & Defense in Depth	0,90
SECFND: Security Concepts	0,90
SECFND: Security Management Part 1	0,80
SECFND: Security Management Part 2	0,50
SECFND: Cryptography	0,90
SECFND: Digital Signatures	1,30
SECFND: SSL/TLS Components	1,00
SECFND: Cryptographic Hashing Algorithms	0,50
SECFND: Cryptographic Encryption Algorithms	1,00
SECFND: Windows Host Terminology	0,60
SECFND: Linux Host Terminology	0,90
SECFND: Endpoint Security	0,50
SECFND: Interpreting Log Data	0,80
SECFND: Network Data Types	1,00
SECFND: Network Data Types and Security Monitoring	0,90
SECFND: Network Monitoring	0,90
SECFND: Next Generation Firewalls	0,40
SECFND: Monitoring Network Protocols	0,90
SECFND: Security Attack Concepts	0,50
SECFND: Network and Web Attacks	0,80
SECFND: Attacks and Evasion	0,90
SECOPS: Analyzing Threat Mitigation Reports	1,50
SECOPS: Scoring with CVSS 3.0	1,50
SECOPS: Securing File Systems	1,30
SECOPS: Identifying Forensic Evidence	1,10
SECOPS: Interpreting Regular Expressions	1,00
SECOPS: Protocol Header Security	1,50
SECOPS: IP Header Security	1,40
SECOPS: ICMP Intrusion	0,90
SECOPS: ICMP Intrusion Part 2	0,90
SECOPS: Transport Layer Headers	1,20
SECOPS: HTTP Headers	1,20
SECOPS: Identifying NetFlow v5 Records	0,90
SECOPS: Examining Intrusion Events	0,40

SECOPS: Intrusion Event Technologies	1,20
SECOPS: Analyzing Intrusion Impact	1,00
SECOPS: Responding to Incidents	1,00
SECOPS: CSIRT Goals and Cybersec Elements	0,90
SECOPS: Data Normalization and 5-Tuple Correlation	0,60
SECOPS: Firepower Management Console and Analysis Methods	0,90
SECOPS: Categorize and Classify Intrusions	1,10
SECOPS: Handling Incident Events and Evidence	1,30
Mentoring Certified Information Systems Security Professional (CISSP)	0,00
Mentoring Systems Security Certified Practitioner (SSCP)	0,00
Oracle Database 11g Release 2: Storage Structures and User Security	1,50
Oracle Database 11g Release 2: Oracle Partitioning and Security Features	2,00
Oracle Database 11g Release 2: Oracle Scheduler and Secure Backup	1,00
Defensive Coding Fundamentals for C#	2,10
Defensive Coding for C#	1,90
Defensive Programming in Android: Input and Methods	1,50
Defensive Programming in Android: Using Standards	1,50
Defensive Programming in Android: Errors, Exceptions, and Testing	1,90
Defensive Programming in Android: Network Access and Java Defensive Techniques	1,60
Thinking Defensively about Functions, Methods, and Input	1,90
Managing Network Interaction	2,20
Errors, Exceptions, and Testing	2,30
Protecting Data in iOS Apps	2,20
Defensive Coding Fundamentals for JavaScript and HTML5	1,70
Defensive Coding for JavaScript and HTML5	1,20
Introduction to Secure Programming	0,70
Secure Programming for C/C++	1,40
Securing C/C++ Applications	1,10
CISA: The Process of Auditing Information Systems - Part 1	1,30
CISA: The Process of Auditing Information Systems - Part 2	1,50
CISA: Governance and Management of IT - Part 1	1,60
CISA: Governance and Management of IT - Part 2	1,50
CISA: Information Systems Acquisition, Development, and Implementation	2,40
CISA: Information Systems Operations, Maintenance, and Service Management	2,30
CISA: Protection of Information Assets - Part 1	1,50
CISA: Protection of Information Assets - Part 2	2,20
Cryptography Fundamentals: Defining Cryptography	1,50
Cryptography Fundamentals: Applying Cryptography	1,80
Securing Mobile Devices in the Enterprise: Mobile Security Threats	2,00
Securing Mobile Devices in the Enterprise: Mobile Security Technologies	1,70
Securing Mobile Devices in the Enterprise: Mobile Security Threat Mitigation	1,60
Securing Mobile Devices in the Enterprise: Configuring Enterprise-level Security	1,30
Attack Vectors and Mitigations	1,40
Vulnerabilities and Exploits	1,00
Android Architecture, Protection, and Development Best Practices	2,70

Android Security Vulnerabilities, Testing, and Enterprise Considerations	2,00
iOS Security Architecture and Application Data Protection	1,50
Securing Against Threats, Securing for Enterprise, and Jailbreaking Devices	1,40
OWASP Overview	1,00
OWASP Top 10: List Item Overview	1,10
OWASP A8 and A3: Cross-Site Attacks	0,90
OWASP A7 and A6: Leaky and Unprepared Applications	1,10
OWASP A4 and A2: Broken Applications	1,20
OWASP A5 and A1: Security and Injection	1,20
OWASP A10 and A9: API and Component Attacks	0,90
CSSLP: Secure Software Concepts	2,20
CSSLP: Secure Software Requirements	1,30
CSSLP: Secure Software Design	2,50
CSSLP: Secure Software Implementation and Coding	2,10
CSSLP: Secure Software Testing	1,50
CSSLP: Software Acceptance, Deployment, Operations, Maintenance, and Disposal	1,40
CSSLP: Supply Chain and Software Acquisition	1,90
Securing User Accounts: Fundamental Security Concepts	2,60
Securing User Accounts: Authorization, Registration, and Passwords	2,10
Securing User Accounts: Logon, Logoff, Account Changes, and Attack Mitigation	1,90
Systems Security Certified Practitioner: Access Controls	1,00
Systems Security Certified Practitioner: Security Operations	0,80
Systems Security Certified Practitioner: Security Administration	0,90
Systems Security Certified Practitioner: Risk Management	0,90
Systems Security Certified Practitioner: Incident Response and Recovery	1,00
Systems Security Certified Practitioner: Cryptography	1,10
Systems Security Certified Practitioner: Network and Communications Security	1,73
Systems Security Certified Practitioner: Systems and Application Security	2,10
Advanced Windows Store Apps with C# in Visual Studio 2013: Security & Optimizing	1,50
Programming in C#: Debugging and Security Implementation	1,10